SHOOK, HARDY & BACON LLP
B. Trent Webb, Esq. (*pro hac vice*)
Peter Strand, Esq. (*pro hac vice*)
Ryan D. Dykal, Esq. (*pro hac vice*)
2555 Grand Boulevard
Kansas City, MO 64108-2613
Telephone: (816) 474-6550
Facsimile: (816) 421-5547
bwebb@shb.com

Robert H. Reckers, Esq. (*pro hac vice*)
600 Travis Street, Suite 1600
Houston, TX 77002
Telephone: (713) 227-8008
Facsimile: (713) 227-9508
rreckers@shb.com

GIBSON, DUNN & CRUTCHER LLP
Mark A. Perry (*pro hac vice*)
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: (202) 955-8500
mperry@gibsondunn.com

Blaine H. Evanson (*pro hac vice*)
Joseph A. Gorman (*pro hac vice*)
Lauren M. Blas (*pro hac vice*)
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 229-7228
bevanson@gibsondunn.com

LEWIS ROCA ROTHGERBER LLP
W. West Allen (Nevada Bar No. 5566)
3993 Howard Hughes Parkway, Suite 600
Las Vegas, NV 89169
Telephone: (702) 949-8200
wallen@lrrlaw.com

RIMINI STREET, INC.
Daniel B. Winslow (*pro hac vice*)
6601 Koll Center Parkway, Suite 300
Pleasanton, CA 94566
Telephone: (925) 264-7736
dwinslow@riministreet.com

John P. Reilly (*pro hac vice*)
3993 Howard Hughes Parkway, Suite 500
Las Vegas, NV 89169
Telephone: (336) 908-6961
jreilly@riministreet.com

Attorneys for Defendants Rimini Street, Inc. and Seth Ravin

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

ORACLE USA, INC., a Colorado corporation; ORACLE AMERICA, INC., a Delaware corporation; and ORACLE INTERNATIONAL CORPORATION, a California corporation,

Plaintiffs,

v.

RIMINI STREET, INC., a Nevada corporation, and SETH RAVIN, an individual,

Defendants.

Case No. 2:10-cv-0106-LRH-PAL

DEFENDANTS RIMINI STREET, INC.'S AND SETH RAVIN'S RULE 50(b) RENEWED MOTION FOR JUDGMENT AS A MATTER OF LAW

Judge: Hon. Larry R. Hicks

Defendants Rimini Street, Inc. and Seth Ravin will and hereby do move for judgment as a matter of law pursuant to Rule 50(b) of the Federal Rules of Civil Procedure on Plaintiffs Oracle International Corporation's and Oracle America, Inc.'s claims under the California Computer Data Access and Fraud Act (Cal. Penal Code § 502); Nevada Revised Statute § 205.4765; the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200); the California Unfair Practices statute (Cal. Bus. & Prof. Code § 17000); unjust enrichment and restitution; and an accounting. There is no legal or legally sufficient evidentiary basis upon which liability or damages can be sustained or imposed on these claims or under these statutes.

This motion is based upon this notice, the attached memorandum of points and authorities, all pleadings, files and records in this action, all testimony and evidence admitted at trial, and on such further argument and evidence as the Court may consider.[1]

DATED: November 13, 2015

GIBSON, DUNN & CRUTCHER LLP

By: *Blaine H. Evanson*
Blaine H. Evanson

Attorneys for Defendants
Rimini Street, Inc. and Seth Ravin

[1] For the convenience of the Court, Rimini is filing this motion separately from its Rule 50(b) motion on Oracle's Copyright Act claims. Rimini notes that the combined page-length of the two motions is 30 pages, consistent with Local Rule 7-4.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

I. INTRODUCTION

"[S]uits under anti-hacking laws have gone beyond the intended scope of such laws and are increasingly being used as a tactical tool to gain business or litigation advantages." *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 F. App'x 498, 506 (3d Cir. 2010). This case presents just such an abusive application of anti-hacking laws, requiring this Court's intervention to protect the legal and constitutional rights of defendants Rimini Street, Inc. and Seth Ravin (collectively, "Rimini"). *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).

This case has always been about copyright infringement: Plaintiffs Oracle America, Inc. and Oracle International Corporation (collectively, "Oracle") complained that Rimini violated the Copyright Act by engaging in specific activities such as local hosting and "cloning" of certain Oracle enterprise software. After this Court ruled that Rimini's activities were outside the scope of the express licenses between Oracle and its customers (and Rimini's clients), the jury found that Rimini's infringement was "innocent" and awarded Oracle $35.6 million as the fair market value of a license to the copyrighted works, while specifically finding that Oracle sustained *zero* lost profits as a result of infringement and Rimini had *zero* infringer's profits. Dkt. 896 at 4-6.

Oracle also maintained that Rimini's use of automated downloading tools for a few months was prohibited by Oracle's website's terms of use and, therefore, amounted to a computer hacking offense under California and Nevada law. Over Rimini's objections, the Court allowed these claims to go to the jury, which found Rimini liable and awarded Oracle $14,400,000 in lost profits and $27,000 in investigation costs. *Id.* at 10-12. As a matter of law, however, the California and Nevada anti-hacking statutes do not outlaw Rimini's use of automated downloading tools in the circumstances proven here; if they did, then those statutes would be unconstitutional on their face and as applied to Rimini's conduct. Moreover, neither the California nor the Nevada anti-hacking statute allows for the recovery of lost profits, and this aspect of the jury's verdict is not supported by legally sufficient evidence. Accordingly, Rimini is entitled to judgment as a matter of law as to both liability and damages on Oracle's claims under the anti-hacking statutes.

As explained below, Rimini is also entitled to judgment as a matter of law on Oracle's claim under the Unfair Competition Law ("UCL"), and the claims Oracle abandoned and failed to prove.

II. BACKGROUND

Oracle has a website where customers can download support materials, directly or through a third party. Rimini used automated download tools to obtain files from that website on behalf of Rimini's clients (who were also Oracle support customers) and with those clients' authorization. Oracle originally encouraged the use of such tools, but then changed the terms of use of its website to prohibit it. From November 2008 to January 2009, Rimini used automated tools in violation of Oracle's terms of use. Rimini stopped using automated tools after January 2009.

A. Oracle's Initial Computer Hacking Allegations

Oracle originally alleged three separate computer hacking claims: (1) violations of four subdivisions of the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(2)(C), (a)(4), (a)(5)(i), & (a)(5)(ii)); (2) violations of four subdivisions of the California anti-hacking statute (Cal. Penal Code § 502(c)(2), (3), (6), & (7)); and (3) violations of four subdivisions of the Nevada anti-hacking statute (Nev. Rev. Stat. § 205.4765(1), (2), (3), & (4)). Dkt. 146 ¶¶ 84-110. Oracle expressly pleaded the Nevada claim "in the alternative, to the extent" Nevada law applied. *Id.* ¶ 102.

B. Evidence Presented At Trial

Oracle America had an online database/website of customer support materials that contained hundreds of thousands of technical support files. 9/22 Tr. 1278:10-13. In general, any given customer was entitled under its license to download thousands of different files from the website. 9/17 Tr. 728:12-22. There was no direct mechanism to download large numbers of files at once; rather, customers had to individually identify and download files. Prior to February 2007, Oracle encouraged the use of automated downloading tools as a means to obtain those files. *Id.* 726:1-11.

Oracle witnesses agreed, consistent with the website terms of use, that customers were allowed to "have consultants access the [Oracle] website on their behalf." 9/18 Tr. 866:9-12 (Allison); *see* 9/22 Tr. 1107:15-19 (same); *id.* 1201:10-13 (Renshaw) (same); *see also* PTX 1569 at 1 (MetaLink Terms of Use) ("the Materials may be shared with or accessed by third parties who are your agents or contractors acting on your behalf"). Rimini's clients authorized Rimini to access Oracle's website and download materials on behalf of the clients. *E.g.*, PTX 482 at 3 (Rimini email to Oracle) ("Our access has been approved by each of our clients, granting access to Metalink3 as

their authorized agents"); 9/17 Tr. 585:8-23. Oracle never contended or presented evidence that Rimini lacked its clients' authorization to access the website. And Rimini downloaded only the specific materials that each client was entitled to download. *E.g.*, 9/16 Tr. 281:23-282:6; *id.* 430:9-18; 9/17 Tr. 555:25-556:10; *id.* 562:21-25; *id.* 567:15-21; *id.* 728:20-22.

Oracle changed its website terms of use on February 19, 2007, to prohibit the use of "any software routines commonly known as robots, spiders, scrapers, or any other automated means to access Customer Connection or any other Oracle accounts, systems or networks." 9/18 Tr. 867:15-869:3; *id.* 768:24-769:3. Rimini subsequently became aware of the change in the website terms of use. 9/16 Tr. 482:11-19; 9/17 Tr. 726:20-21; PTX 20.

During a three-month period, from November 2008 to January 2009, Rimini on occasion used automated tools to download support materials. 9/22 Tr. 1194:7-15. Rimini maintained its policy of downloading only materials to which specific clients were entitled (9/17 Tr. 726:1-24), and "made all sorts of arrangements" to "minimize the impact on Oracle servers," including "work[ing] on nights and weekends around … the peak periods" and "purposely slow[ing] down the archive." 9/18 Tr. 771:3-18. As Mr. Ravin explained, "[t]here was no benefit for [Rimini] to crash a server" when Rimini was "trying to get information from" it. *Id.* 771:19-23. "The intent [wa]s not to create undue burden on [Oracle's] servers, but to provide Oracle customers with a simpler mechanism to obtain all of the online content they are entitled to." PTX 482 at 3.

Oracle nonetheless blocked Rimini's IP addresses to prevent Rimini from using automated download tools to obtain support materials that Rimini's clients were legally entitled and authorized to have a third party obtain on their behalf. *E.g.*, 9/22 Tr. 1175:17-1176:3 (Hicks); 1232:8-1233:1 (Baron). Rimini obtained additional IP addresses so that it could obtain support materials that customers "were entitled to get." 9/22 Tr. 1232:8-20 (Baron).

After January 2009, Rimini stopped using automated tools for downloads (9/17 Tr. 583:23-584:1, 726:25-727:7), and there is no allegation or evidence that Rimini engaged in automated downloading after January 2009. *E.g.*, 9/22 Tr. 1194:11-15 (Hicks) (agreeing there was "no evidence that Rimini" used prohibited automated tools "other than in those three months").

Mr. Hicks testified that Rimini's automated downloading during the three-month window at

issue caused "database deadlocks" and a "slow-down effect." 9/22 Tr. 1172:9-15. There was conflicting evidence about the extent of the slowdown (*see* 9/22 Tr. 1185:25-1186:8; 9/29 Tr. 2295:1-4; *id.* 2356:15-18), but nothing in this motion requires the Court to resolve that dispute between the parties' experts. Additionally, on one occasion "in the middle of the night Pacific time" in January 2009, the automated downloading caused Oracle's servers to go down for more than three hours. 9/22 Tr. 1194:24-1195:14. Oracle "resolved that problem by rebooting the server." *Id.* 1195:12-14.

Witnesses on both sides agreed that the automated downloading did not cause any physical harm to Oracle's computers or servers. 9/22 Tr. 1194:20-23 (Hicks); *id.* 1219:4-7 (Renshaw); 9/29 Tr. 2306:1-2 (Klausner) ("There was no damage done"); *id.* 2305:6-13; *id.* 2306:14-17 ("reboot[ing] the system" is "different than impair," because "it comes back up and everything is okay").

Oracle's damages expert, Elizabeth Dean, opined that Oracle had incurred $27,000 in "labor costs for actual Oracle employees for short durations of time in November, December of 2008 and January of 2009, when they were investigating why the computer systems were stalling or deadlocking." 9/24 Tr. 1831:3-13. With the exception of this specific amount, Oracle did not attempt at trial to quantify, calculate, or claim any damages caused by the automated downloading, including specifically the deadlocks, slow-downs, or the one instance when the server had to be rebooted. *E.g.*, 9/22 Tr. 1186:23-1187:8 (stating only that there was a "negative impact").

Ms. Dean also opined that Oracle had sustained $14.4 million in "lost profits" related to the automated downloading, calculated as follows: She took the customer IDs that Rimini used for automated downloading in November 2008 to January 2009, and then isolated those customers in her overall copyright damages lost profits analysis. 9/24 Tr. 1832:21-1833:12. As Ms. Dean explained, if those specific customers were "not in the lost profits" analysis, she "didn't add anything," but "in the instance that [she] was already claiming lost profits for them, they accumulate to that $14.4 million." *Id.* 1833:6-12; *id.* 1833:13-19 (Ms. Dean agreeing with the characterization that "[i]f the jury were to conclude that the appropriate measure of damages for the automated downloading would relate to the customers whose IDs were used, [her] opinion would be the damages should be 14.4 million"). In other words, Oracle claimed the *exact same* lost profits for the *exact same* customers as a result of both copyright infringement and automated downloading, and made no attempt to tie the

lost profits calculation to Rimini's automated downloading activities.

There was also evidence presented at trial regarding what "hacking" a computer means. Edward Screven, who is "in charge of security at Oracle" (9/23 Tr. 1542:15), explained that hackers are those who "attack[]" and "make money by breaking into systems" (9/23 Tr. 1552:1-19); "[t]hey steal credit card numbers and sell them" (*id.*); "[t]hey get sensitive company information and use it for financial gain" (*id.*); they "break into systems" (*id.* 1552:8-9; *id.* 1548:13-1549:19 (same)); they "exploit" "vulnerabilities in the software" (*id.* 1551:1-6); they "penetrate through firewalls" (*id.* 1557:15-1558:6); and they send "poison email messages that set up relay stations that let them get into your networks" (*id.*). He did not testify that Rimini engaged in any of these hacking activities.

C. Oracle Abandons Most Of Its Hacking Allegations

Rimini repeatedly briefed the legal unavailability of Oracle's computer hacking claims. *E.g.*, Dkt. 741 at 21-24; Dkt. 766 at 59-61; Dkt. 773 at 16-19; Dkt. 838 at 13-18. Rimini consistently argued that as a matter of law it could not be held liable or ordered to pay damages under any of the provisions of the federal, California, or Nevada anti-hacking statutes pleaded in Oracle's complaint.

In response to Rimini's challenges, Oracle began to drop its hacking claims. First, when briefing jury instructions, Oracle dropped its claims under subsection (a)(4) of the federal law, subsection (c)(7) of the California law, and subsections (2) and (4) of the Nevada law. Dkt. 752 at 66-87. Oracle then dropped its claim under the federal statute *in its entirety* just before the case went to the jury, as well as the breach of contract and trespass to chattels claims premised on the same conduct. 10/6 Tr. 3341:18-19. As a result, after originally alleging twelve different violations of three different laws (plus breach of contract and trespass), Oracle ultimately withdrew all but four of its computer hacking theories under two state laws. The jury was therefore instructed (over Rimini's objection (*e.g.*, Dkt. 766 at 59-61; Dkt. 838 at 13-18)) on sections (c)(2) and (c)(3) of the California law and sections (1) and (3) of the Nevada law. Dkt. 880 (Instruction Nos. 47, 48, 49, 53, & 54).

D. Jury Verdict

The jury returned a verdict on October 13, 2015, in which it found that Rimini had violated the California and Nevada anti-hacking statutes. The jury awarded $8,827,000 to Oracle America and $5,600,000 to Oracle International Corporation under each statute. Dkt. 896 at 10-12. That

figure is exactly the $14,400,000 in lost profits, plus the $27,000 in investigation costs, presented by Oracle (through Ms. Dean) at trial. Consistent with Ms. Dean's testimony that the $14.4 million of lost profits was entirely duplicative of her copyright damages analysis, the jury divided the $14.4 million by the same allocation Oracle requested for copyright infringement lost profits: "Oracle America gets 61 percent … and Oracle International Corporation gets 39 percent as a payment for the copyrights." 9/24 Tr. 1806:18-21 (Dean). Sixty-one percent of $14.4 million is $8,784,000 and 39 percent is $5,616,000—the figures the jury returned, with the same rounding urged by Oracle's counsel. *See* 10/6 Tr. 3494:12-24 (Oracle closing argument) (asserting the computer damages should be awarded as "8.8" for Oracle America and "5.6 million" for Oracle International). The jury then awarded the $27,000 investigation costs to Oracle America. The jury also found that Oracle International Corporation did not lose any profits as a result of infringement. Dkt. 896 at 4.

III. LEGAL STANDARD

Judgment as a matter of law is warranted when "the evidence, construed in the light most favorable to the nonmoving party, permits only one reasonable conclusion that is contrary to the jury's verdict." *Reiber v. City of Pullman*, 613 F. App'x 588, 590 (9th Cir. 2015). Neither a finding of liability nor a damages award may be sustained when there was not legally sufficient evidence at trial to support it. *E.g.*, *id.* at 591 ("the evidence at trial was insufficient, as a matter of law" to sustain finding of liability); *Yacht West, Ltd. v. Christensen Shipyards, Ltd.*, 464 F. App'x 626, 628 (9th Cir. 2011) ("Substantial evidence did not support the jury's award of" compensatory damages).

The California anti-hacking statute provides, in relevant part:

> (c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:
>
> ….
>
> (2) Knowingly accesses and *without permission takes, copies, or makes use of any data* from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and *without permission uses or causes to be used* computer services.
>
> ….
>
> (e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may

> bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. *Compensatory damages shall include* any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.

Cal. Penal Code § 502 (emphases added). The statute defines, *inter alia*, "access," "computer network," "computer services," "computer system," "data," and "injury." *Id.* § 502(b).

The Nevada anti-hacking statute provides, in relevant part:

> **205.4765 Unlawful acts regarding computers: Generally**
> 1. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization: (a) Modifies; (b) Damages; (c) Destroys; (d) Discloses; (e) Uses; (f) Transfers; (g) Conceals; (h) Takes; (i) Retains possession of; (j) Copies; (k) Obtains or attempts to obtain access to, permits access to or causes to be accessed; or (l) Enters, → data, a program or any supporting documents which exist inside or outside a computer, system or network is guilty of a misdemeanor.
> ….
> 3. Except as otherwise provided in subsection 6, a person who knowingly, willfully and without authorization: (a) Destroys; (b) Damages; (c) Takes; (d) Alters; (e) Transfers; (f) Discloses; (g) Conceals; (h) Copies; (i) Uses; (j) Retains possession of; or (k) Obtains or attempts to obtain access to, permits access to or causes to be accessed, → a computer, system or network is guilty of a misdemeanor.
> ….
> **NRS 205.511 Victim authorized to bring civil action**.
> 1. Any victim of a crime described in NRS 205.473 to 205.513, inclusive, may bring a civil action to recover:
> (a) Damages for any response costs, loss or injury suffered as a result of the crime;
> (b) Punitive damages; and
> (c) Costs and reasonable attorney's fees incurred in bringing the civil action.

Nev. Rev. Stat. §§ 205.4765, 205.511. The statute defines, *inter alia*, "access," "computer," "data," "network," "response costs," and "system." *Id.* §§ 205.4732-205.476.

IV. ARGUMENT

Rimini's use of automated downloading tools from November 2008 to January 2009, even if in violation of Oracle's website terms of use, does not as a matter of law constitute criminal computer hacking upon which the jury's liability or damages verdicts may be sustained, for several reasons:

As a starting point, Oracle cannot invoke either California or Nevada state law against Rimini. Oracle International Corporation lacks standing to sue under these statutes, because Rimini never accessed a computer or website owned by Oracle International Corporation. And Oracle failed to introduce into evidence any predicate facts identifying where the conduct occurred or where the

affected servers were located. Without this evidence, there is no basis upon which to conclude that California or Nevada law can be applied under choice-of-law principles or the Commerce Clause.

Even if the statutes were applicable, the liability verdict cannot stand as a matter of law. Oracle's argument at trial was that Rimini violated the website terms of use when it used automated download tools rather than clicking individually on each file, but the statutes do not prohibit automated downloading or in any way criminalize the means of accessing information on a computer. There was no dispute at trial that Rimini had Oracle's permission and authorization to obtain support materials on behalf of its clients, and that Rimini had its clients' permission to access the website and obtain those materials on the clients' behalf. As a result, Rimini's use of automated downloading does not violate the plain terms of the statute and Rimini's access of the website was specifically authorized. Particularly when viewed under the rule of lenity and the canon of constitutional avoidance, Rimini's conduct was not unlawful as a matter of law.

If the anti-hacking statutes could be construed to reach Rimini's conduct, then they would be unconstitutional—on their face, and particularly as applied here. The relevant language, drafted in the 1980s in a time that bears no resemblance to the modern technological environment, is void for vagueness. The statutes are also unconstitutional as applied to Oracle's theory that a violation of website terms of use creates liability, for reasons the en banc Ninth Circuit has explained at length in the context of the federal anti-hacking statute. *See Nosal*, 676 F.3d at 859-64. The Constitution does not permit application of state law to situations that federal law cannot reach.

Even if the liability verdict under the anti-hacking statutes could withstand legal and constitutional scrutiny, $14.4 million of the damages award should be stricken as a matter of law. Neither statute authorizes the recovery of lost profits. And even if they did, Oracle's theory of lost profits is without legally sufficient basis in the evidence because (among other defects) Oracle did not contend, much less prove, that even one customer joined Rimini because of automated downloading.

In addition to correcting the erroneous and unsupportable liability and damages verdicts on the hacking claims, the Court should grant judgment as a matter of law on Oracle's UCL claim.

A. Neither California Nor Nevada State Anti-Hacking Law Applies To Rimini's Conduct

The trial record does not support the jury's finding of liability under the California *or* Nevada

anti-hacking statutes because Oracle International Corporation does not even own the servers that were the subject of the alleged conduct, and because Oracle did not prove where the conduct occurred, and therefore cannot establish that either California's or Nevada's law applies.

1. Rimini Did Not Access Oracle International Corporation Computers

Oracle presented no evidence at trial that Oracle International Corporation was the "owner or lessee" of computers accessed by Rimini (Cal. Penal Code § 502(e)) or the "victim" of unauthorized access by Rimini (Nev. Rev. Stat. § 205.511(1)). Instead, the trial evidence established that the Oracle support website that was the subject of the anti-hacking claims belonged to Oracle America. *E.g.*, 9/24 Tr. 1772:18-1773:3 ("Oracle America provides the direct support services to the customers"). Accordingly, Oracle International Corporation lacks standing under the statutes to pursue a claim. *See*, *e.g.*, *In re Google Android Consumer Privacy Litig.*, 2013 U.S. Dist. LEXIS 42724, at *20-21 (N.D. Cal. Mar. 26, 2013) (no anti-hacking standing with no injury). Rimini made this argument in its Rule 50(a) motion (Dkt. 838 at 13 n.3); Oracle failed to respond, and thus has conceded this point. As a result, the verdict on the anti-hacking claims must be reduced by $5.6 million (the amount awarded by the jury to Oracle International Corporation).

2. Oracle Failed To Prove Which (If Any) State Law Applies

Oracle did not introduce evidence at trial establishing where Rimini's conduct occurred or where Oracle's servers were located. Under choice-of-law principles, the Commerce Clause, and the extraterritoriality doctrine, there is no basis in the record upon which the Court can determine whether California's or Nevada's computer crime laws can be applied.

Evidence introduced at trial showed that Rimini had "data centers" and servers in "California and North Carolina" (9/17 Tr. 525:20-25, 574:11-16) and the servers moved at some point from California to Las Vegas (and some remain in North Carolina) (*id.* 602:3-7); "very few of Rimini's top executives are actually based … in Las Vegas" (9/23 Tr. 1393:9-12); Rimini began with employees working in California, North Carolina, Washington D.C., and Chicago (9/17 Tr. 691:17-692:7); and Rimini's support engineers are all over the world, including Colorado, Florida, Romania, India, Europe, and Singapore (9/22 Tr. 1297:3-6; 9/25 Tr. 2032:4-9). Oracle is headquartered in California (9/21 Tr. 910:1-2), but is "a global company" with "customers worldwide that are accessing the

[online] knowledge documentation" (9/22 Tr. 1204:15-17). Oracle has "over 130,000 employees worldwide" (9/21 Tr. 951:11-12) and a "global technical support team" of "over 8,000 engineers" (9/22 Tr. 1293:12-17). David Renshaw first noticed and investigated Rimini's automated downloading in November 2008 from the *United Kingdom*. *Id.* 1198:22-23, 1200:24-1201:2. There was *no* evidence introduced at trial regarding the physical location of the affected servers.

In this context, where the companies have servers distributed across the United States and employees working around the world, the lack of evidence regarding the location of conduct or servers creates unresolvable choice-of-law issues. The accused conduct could have been a Rimini employee in Florida using a Kansas client's ID to access an Oracle server in Texas (in fact, Oracle's prior interrogatory responses in this case assert that the affected servers were in Texas and Colorado, and reference the use of a Kansas client's ID). In such a scenario, neither California nor Nevada law could apply to Oracle's claims. *See*, *e.g.*, *GMC v. Eighth Judicial Dist. Court of Nev.*, 122 Nev. 466, 478 (2006) (Arizona law could not be applied when there was "no relationship with Arizona").

It is insufficient for Oracle to argue that California *or* Nevada law applies, plead them in the alternative, and then just move on with its case—there must be facts in the record establishing that one or the other state's law *actually* applies. *See id.* at 473 (Nevada choice-of-law doctrine requires identifying state with "the most significant relationship to the occurrence and the parties"). With no evidence regarding the location of the conduct or servers, the Court cannot even conduct a proper choice-of-law inquiry to determine which state's law—whether California, Nevada, or some other state—applies. *See id.* at 478 (holding that Arizona law did not apply to one defendant because there was "no relationship with Arizona," but did apply to another defendant because "Arizona has a more significant relationship" than Nevada). Oracle had the burden to establish which law applied, and its failure to elect either law before submitting the case to the jury demonstrates that Oracle failed to meet that burden and now precludes Oracle from recovering under either law at all. Even at this point, *after* the return of the jury's verdict, Oracle has not attempted to demonstrate which state's law applies. Under Oracle's approach, it would be permissible to plead in the alternative laws of all *fifty* states to see which ones the jury might find violated so that Oracle could attempt to recover damages.

Indeed, applying either California or Nevada law without any evidence establishing either

state's basis for regulating the asserted conduct would be unconstitutional. "No State can legislate except with reference to its own jurisdiction. … Each State is independent of all the others in this particular." *Bonaparte v. Tax Court*, 104 U.S. 592, 594 (1881). "[O]ne State's power to impose burdens on the interstate market … is also constrained by the need to respect the interests of other States." *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571-72 (1996) (citing *Gibbons v. Ogden*, 9 Wheat. 1, 194-96 (1824) and *Healy v. Beer Institute*, 491 U.S. 324, 335-36 (1989)). Thus, "the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State." *Healy*, 491 U.S. at 336 (quotations and citations omitted). In short, without the necessary evidence establishing the location of the conduct, Oracle's attempt to apply California or Nevada law runs afoul of the Commerce Clause because Oracle seeks the application of one state's law to conduct that may have occurred wholly outside of that state's borders.

Importantly, different states have different laws regulating computer hacking. *See*, *e.g.*, Susan W. Brenner, 2 Data Sec. & Privacy Law § 15:22 ("Every state has some sort of prohibition against accessing a computer, computer system, or network without authorization" but "there is little consistency in the way the offense is characterized"). These differences are important because "no single State … [can] impose its own policy choice on neighboring States," and one state cannot "impose sanctions on [a defendant] in order to deter conduct that is lawful in other jurisdictions." *Gore*, 517 U.S. at 571-73; *see also Phillips Petrol. Co. v. Shutts*, 472 U.S. 797, 814-23 (1985). Even the two state laws here criminalize different conduct. *See infra* Section IV.B.

And even if some of the conduct occurred in California or Nevada, there is no principled basis on which this Court could determine the extent of the conduct in either state. Oracle alleged that "[a]t least some of Defendants' unlawful conduct … occurred at Rimini Street's operations in Nevada" and pleaded the Nevada claim in the alternative "to the extent the Court may determine that NRS 205.4765 applies to such conduct in Nevada." Dkt. 146 ¶ 102. But there is no basis in the record for apportioning damages based on conduct that occurred in California, Nevada, or anywhere else. This renders the damages award so speculative as to be unsupportable as a matter of law.

Until the day before the case was sent to the jury, Oracle was pressing a *federal* hacking claim

for which no choice-of-law analysis was necessary. Its decision to drop that claim brings into sharp focus Oracle's own failure to prove which (if either) of its surviving state law theories could be applied to the challenged conduct. And its failure to prove *any* predicate for this critical choice-of-law point is fatal to its claims under both California and Nevada law. Indeed, as Rimini has argued throughout, the state law claims are no more supportable than the federal claim. Oracle dropped its federal claim only after the Court correctly ruled that lost profits are not recoverable (Final Jury Instructions, sent via email Oct. 5, 2015) in an apparent attempt to seek the same impermissible recovery where there was less case law in the way. But, as set forth throughout this motion, Oracle's gamble to pursue only state law claims cannot be supported as a matter of law.

B. Rimini's Conduct Did Not Violate The Anti-Hacking Statutes As A Matter Of Law

Rimini did not violate the California or Nevada anti-hacking statutes as a matter of law because neither statute prohibits the use of automated download tools. The mere fact that Rimini violated Oracle's website terms of use is not a cognizable claim under either statute—particularly where Rimini had the authorization of Oracle and Rimini's clients to access the website.

As Oracle recognizes, "both the [California] and the [Nevada anti-hacking statutes] are criminal statutes." Dkt. 900 at 19. Although the statutes also authorize civil claims, the Ninth Circuit has held squarely that the interpretation of these statutes must be guided by principles of criminal law. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009); *see Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). Accordingly, the rule of lenity applies, and the anti-hacking statutes must "be construed strictly." *Nosal*, 676 F.3d at 863 (citation omitted). Any "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Brekka*, 581 F.3d at 1134 (citation omitted). "If there is any doubt about whether Congress intended [the statute] to prohibit the conduct in which [the defendant] engaged, then [the court] must choose the interpretation least likely to impose penalties unintended by Congress." *Nosal*, 676 F.3d at 863 (citation omitted).

Moreover, "[i]t is a cardinal principle of statutory interpretation … that when an Act of Congress raises a serious doubt as to its constitutionality, [a court] will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided." *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (quotations and citations omitted). As set forth below, there are

serious constitutional concerns with both states' anti-hacking statutes, particularly in the way Oracle attempts to apply them here. The canon of constitutional avoidance requires the Court to interpret the statutes in a way that avoids those serious constitutional questions. *See*, *e.g.*, *Cherokee Nation v. Leavitt*, 543 U.S. 631, 646 (2005) (when two interpretations of a statute are "reasonable," avoiding constitutional doubts "tips the balance against" an interpretation that "may violate the Constitution"); *Zadvydas*, 533 U.S. at 689 (reading into an immigration statute an "implicit limitation" not found in the text to avoid constitutional problems); *Crowell v. Benson*, 285 U.S. 22, 62 (1932).

The two statutes prohibit different types of conduct. The Nevada law prohibits either *accessing* a computer system or *using* data taken from the computer system, if either action is taken "without authorization." Nev. Rev. Stat. § 205.4765(1)(e) ("Uses"), (1)(k) ("Obtains or attempts to obtain access to…"); *id.* § 205.4765(3)(i), (k) (same). Sections (2) and (3) of the California law, in comparison, criminalize the *use* of data (if undertaken "without permission"), not the *access* to a computer. Cal. Penal Code § 502(c)(2) ("Knowingly accesses and without permission, takes, copies, or makes use of any data…"); *id.* (c)(3). "A plain reading of the [California law] demonstrates that its focus is on unauthorized taking or use of information." *United States v. Christensen*, 801 F.3d 970, 994 (9th Cir. 2015).[2]

Applying the rule of lenity and resolving ambiguities in favor of limiting liability, it is clear that the statutes do not criminalize Rimini's conduct, for several reasons.

First, neither statute prohibits the *means* by which one accesses a computer or otherwise specifies that use of an automated downloading tool is criminally unlawful. Oracle does not dispute that Rimini had authorization to access the information that Rimini downloaded from Oracle's website. *See*, *e.g.*, 9/18 Tr. 866:9-12; 9/22 Tr. 1107:15-19, 1201:10-13; PTX 1569. The only question was whether Rimini was permitted to do so with an automated downloading tool. But

[2] When the California Legislature passed the law in 1987, it made a distinction between access and use. *See* Request for Judicial Notice ("RJN"), Ex. 3 at 2 (S.B. 255, Bill Analysis (Cal. Feb. 27, 1987)) (describing section 2 as prohibiting "taking or copying data" and section 3 as "unauthorized use of computer services" whereas sections 1, 4, 6, and 7 prohibit different types of "access"); *id.* Ex. 5 at 2-3 (S.B. 255, Bill Analysis, Assemb. Comm. on Public Safety (Cal. June 1, 1987)) (the law created one category of "penalties for 'hackers,'" which is "one who *accesses* a computer" and a separate category of "penalties for unauthorized *use*") (emphases added).

because nothing in either anti-hacking statute prohibits using a tool for downloading information in a way that is prohibited by a website's terms of use, this claim fails as a matter of law.

Oracle argued at trial that Rimini violated the website terms of use when it accessed Oracle's website using the automated download tools. *E.g.*, 10/6 Tr. 3493:4-12 (Oracle closing argument) ("the computer access claims" are "about" "the automated downloading going onto our system without permission"). Oracle blocked Rimini's IP address specifically to prevent Rimini from using automated tools. *E.g.*, 9/24 Tr. 1759:5-12 (Whittenbarger) ("Q. … Oracle blocked that IP address in response to the massive download volumes? A. Probably, yes. Q. Did you later learn that Oracle, you know, told Rimini Street that very directly? A. Yes, I was aware of that."). Had Rimini clicked on the exact same files one by one (rather than used automated tools), Oracle acknowledges that Rimini would not be liable under the anti-hacking statutes. *E.g.*, 9/17 Tr. 724:4-725:11 (Rimini could have "download[ed] manually one by one, click, click, click").

But nothing in the plain language of the statutes criminalizes the particular *means* of access that may or may not be permitted by a website's terms of use. The statutes do not mention methods of access, automated downloading tools, or website terms of use. Rather, the *only* basis for liability is if an individual has no right to access the website or use the information at all. Indeed, even when a defendant purposefully installs software that circumvents technical barriers to secretly transmit data, there is no liability because the defendant had some permission to access the plaintiff's computer when the plaintiff installed the file, and the additional unauthorized activity did not establish access without permission. *See*, *e.g.*, *Flextronics Int'l, Ltd. v. Parametric Tech. Corp.*, 2014 U.S. Dist. LEXIS 73354, at *15 & n.46 (N.D. Cal. May 28, 2014) ("[B]ecause [plaintiff] voluntarily gave permission to install some portion of [defendant's] software on its computers, any additional code installed at the same time was also installed with permission. This argument has been adopted in many other cases.") (collecting cases); *In re iPhone App. Litig.*, 2011 U.S. Dist. LEXIS 106865, at *40 (N.D. Cal. Sept. 20, 2011) ("the iOS and third party apps—which contain the alleged 'surreptitious code'—were all installed or updated *voluntarily* by Plaintiffs") (emphasis in original).[3]

[3] Although some courts have held under the California anti-hacking statute that "accessing or using a computer, computer network, or website in a manner that overcomes technical or code-based

Oracle never claimed that Rimini was not allowed to access the website *at all*—to the contrary, the testimony and documents established that Rimini *was authorized* to access the website. *E.g.*, 9/18 Tr. 866:9-12; 9/22 Tr. 1107:15-19; *id.* 1201:10-13; PTX 1569. Indeed, it is undisputed that Rimini continued to download and obtain client support materials from Oracle's website before, during, and after the time period at issue. *E.g.*, 9/18 Tr. 772:23-25 ("Oracle ultimately allow[ed] Rimini Street to complete the project" of downloading support files for a customer at the time Rimini was using prohibited automated download tools). The conduct Oracle points to as a violation of the anti-hacking statutes—the automated downloading tools—is not prohibited under the plain terms of either of these *criminal* statutes, and therefore cannot as a matter of law support the jury's verdict.

Second, Rimini *had permission and authorization* to access the website from the clients, which precludes liability under either anti-hacking statute as a matter of law.

Oracle's argument to the jury was premised on a clear error of law. Oracle acknowledged that Rimini had permission from its clients to access Oracle's website, but argued to the jury that Rimini needed *Oracle's* permission and that without *Oracle's* permission, Rimini's conduct violated the anti-hacking statutes. *See* 10/6 Tr. 3629:8-11 (Oracle closing argument) ("I told you about that when I went through the jury instructions. It's not the clients authorizing it. It's did Oracle authorize you to come on the computer. Answer, no.").

Contrary to Oracle's argument, the statutes do not require the permission of the owner of the computer. They simply require "authorization" or "permission." Neither statute defines those terms. Nor do they define *whose* permission or authorization is required. But the Ninth Circuit in *Nosal* held expressly that a defendant does not act "without authorization" where it has permission or authorization to access the computer from someone with valid credentials. 676 F.3d at 863-64. It is undisputed that this was true of Rimini's access here. *E.g.*, PTX 482; 9/17 Tr. 585:8-23. And the Ninth Circuit's interpretation, based on the rule of lenity and constitutional avoidance, applies

---

barriers is 'without permission'" (*Facebook, Inc. v. Power Ventures, Inc.*, 2010 U.S. Dist. LEXIS 93517, at *35 (N.D. Cal. July 20, 2010)), that line of analysis precedes and is inconsistent with the Ninth Circuit's published decision *United States v. Christensen*, 801 F.3d 970, which makes clear that the "without permission" language in section 502(c)(2) of the law focuses on subsequent *use* of information, not the "access" of the website. *Id.* at 993-94. And, in any event, Rimini did not overcome technical barriers by simply obtaining additional IP addresses.

squarely to the California and Nevada anti-hacking statutes.[4]

In *Brekka*, the Ninth Circuit interpreted the term "authorization" in the federal anti-hacking law to mean "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." 581 F.3d at 1135. There, the defendant "was given permission to use [his employer] LVRC's computer" and therefore had authorization to access the computer. *Id.* Similarly, in *Nosal*, the defendant convinced current employees of his former company to use their log-in credentials and send him confidential information from the company's computers. 676 F.3d at 856. The en banc Ninth Circuit held that "[b]ecause Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of 'without authorization, or exceeds authorized access.'" *Id.* at 864. Those interpretations were compelled by the rule of lenity and the canon of constitutional avoidance (*Nosal*, 676 F.3d at 863; *Brekka*, 581 F.3d at 1134-35), are binding here, and must be applied to the state laws because those statutes are subject to the same constitutional constraints as the federal law.

That interpretation is consistent with a separate provision in the California law, which states that "[s]ubdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment." Cal. Penal Code § 502(h)(1). As that section demonstrates, the Legislature did not intend to criminalize actions taken when the actor believed he had permission.

The expansive interpretation offered by Oracle would extend to an incredibly broad swath of conduct that the California and Nevada Legislatures never intended to criminalize.[5] For example,

---

[4] Rimini requested that the jury be instructed for the California law that "[a]n individual does not act 'without permission' if he uses a third party's credentials to access a website that the third party has authorization to access to obtain material authorized by the third party" (*e.g.*, Dkt. 868 at 98), and similarly for the Nevada law (*id.* at 106). That request was not adopted.

[5] The Nevada Legislature clearly intended to circumscribe the scope of conduct prohibited by the Nevada anti-hacking law. *See* RJN Ex. 6 at 4 (Minutes, Assemb. Comm. on Jud. (Nev. Apr. 22, 1983)) ("one question which [the bill] does raise is how you define 'authorization, right to use', etc. … [T]hese are very ambiguous terms"); *id.* at 5 ("interested in limiting, to a certain extent, a statute which may apply to computers. … [I]f the law is made too direct to computers and too general, then computers are handled as special things under the law and this should not be"); *id.* ("this bill should not be allowed to become too general or all encompassing").

under Oracle's interpretation, a husband who logged in to his wife's email with her permission but contrary to Gmail's terms of use would be a criminal. A girlfriend who posted through a boyfriend's Facebook page at his request but contrary to Facebook's terms of use would be a criminal. A new law firm associate who used a 3L friend's Westlaw password to do a little research would be a criminal. An employee checking ESPN contrary to his employer's computer terms of use would be a criminal. This Court should not apply such a sweeping interpretation to a criminal law. *See Nosal*, 676 F.3d at 859 ("While ignorance of the law is no excuse, we can properly be skeptical as to whether Congress, in 1984, meant to criminalize conduct beyond that which is inherently wrongful").

Third, sections 502(c)(2) and (3) of the California anti-hacking statute criminalize *using* data or computers without permission, not *accessing* a website without permission. Cal. Penal Code § 502(c)(2), (3); *Christensen*, 801 F.3d at 994. Yet Oracle's evidence at trial related only to *access* of its website. Oracle never contended or presented evidence that Rimini committed computer hacking because of the way it subsequently *used* the data. For example, Oracle did not claim that Rimini violated these statutes because it took, copied, or made use of the downloaded materials in violation of the website terms of use. As a result, Oracle's claim under California law fails as a matter of law.

Fourth, Oracle is trying to transform a breach-of-contract claim into computer hacking liability by seizing on expansive language in the anti-hacking statutes. Oracle pleaded a breach-of-contract claim (Dkt. 146 ¶¶ 111-115), but dropped it before sending the case to the jury (Dkt. 852 at 2). Oracle thus contends that conduct that does not even amount to a civil breach of contract is *criminal* hacking. Oracle's argument is incorrect as a matter of law and violates fundamental policies underlying commercial and consumer transactions.

Companies can include terms of use in their websites and if someone violates those terms, the operator of the website has a remedy at law in the form of a breach-of-contract action—just as Oracle pleaded in this case. But, when enacting anti-hacking legislation, Congress and state legislatures did not intend to criminalize consumer deviations from website terms of use. *See Nosal*, 676 F.3d at 859 (interpreting federal anti-hacking statute as criminalizing violations of terms of use "would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime"). Such an application of anti-hacking laws would turn "millions of unsuspecting

individuals" into criminals by "transform[ing] whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 859-60.

More generally, courts reject attempts to inject tort or statutory liability into commercial situations governed by the law of contract: "expand[ing] tort liability to allow for a tortious breach of contract as long as the breach violates a statute" is a "novel proposition" that "fails to consider the dangers implicit in such a radical departure from well-established limits to commercial recovery." *JRS Prods., Inc. v. Matsushita Elec. Corp. of Am.*, 115 Cal. App. 4th 168, 182 (2004). The "essential nature of the conduct" is what determines "the appropriate cause of action"—when, like here, that conduct is "fundamentally" contractual, then "the *very same activity*" cannot be bootstrapped into an independent claim. *Id.* at 182-83 (emphasis in original); *see Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 514 (1994) ("a party to a contract … cannot be bootstrapped into tort liability by the pejorative plea of conspiracy"); *Arntz Contracting Co. v. St. Paul Fire & Marine Ins. Co.*, 47 Cal. App. 4th 464, 479 (1996) ("A contracting party's unjustified failure or refusal to perform is a breach of contract, and cannot be transmuted into tort liability by claiming that the breach detrimentally affected the promisee's business").

Thus, allowing hacking claims to be based on a breach of contract for violating a website's terms of use—particularly when, as here, the party does not even pursue its breach-of-contract claim—would impermissibly displace the settled common law governing contractual relations and criminalize private and commercial behavior. This is a dramatic and unsupportable application of statutes intended to address computer hacking, not routine online interactions. *See Nosal*, 676 F.3d at 857 ("Congress acts interstitially, [and] we construe a statute as displacing a substantial portion of the common law only where Congress has clearly indicated its intent to do so"). Oracle's illegitimate pursuit of these claims raises the very concern identified by the U.S. Court of Appeals for the Third Circuit in a case involving the California anti-hacking statute: "[S]uits under anti-hacking laws have gone beyond the intended scope of such laws and are increasingly being used as a tactical tool to gain business or litigation advantages." *RCM Digesters, Inc.*, 409 F. App'x at 506.

C. The Relevant Statutory Provisions Are Unconstitutional Facially And As Applied

If the California and Nevada anti-hacking statutes governed *access*, regulated the *means* of

access, required *Oracle's* permission for the means of access, and could be applied legitimately in place of a breach-of-contract claim, they would be unconstitutional both facially and as applied.

1. The Statutory Provisions Are Void For Vagueness On Their Face

"[T]he void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). If a statute does not meet both of these requirements, then it "fails to meet the requirements of the Due Process Clause." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999) (quoting *Giaccio v. Pennsylvania*, 382 U.S. 399, 402-03 (1966)); *see Johnson v. United States*, 135 S. Ct. 2551, 2556 (2015) ("Our cases establish that the Government violates [due process] by taking away someone's life, liberty, or property under a criminal law so vague that it fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement").

The four provisions at issue are unconstitutionally vague in their entirety because they do not define the offense with sufficient definiteness and they allow for arbitrary enforcement. The statutes use expansive language written thirty years ago to criminalize conduct in a world that bears no resemblance to the modern technological world. Even if their language applied to a sufficiently narrow and decipherable set of conduct in the 1980s, in the modern age they create an unlimited minefield of criminal responsibility for any person or company that uses a computer.

The Nevada statute was enacted in 1983 and the California statute was enacted in 1987. *See* A.B. 133, Nev. Stats. 1983, c. 456 (1983); S.B. 255, Cal. Stats. 1987, c. 1499 (1987). The language in subsections 502(c)(2) and (3) of the California law remains untouched from 1987. *See* S.B. 255, Cal. Stats. 1987, c. 1499 (1987). The language of subsections (1) and (3) of the Nevada law is the same in format, but has had more verbs added to the prohibited acts. *See* A.B. 133, Nev. Stats. 1983, c. 456 (1983). At that time, committing a prohibited computer act essentially required physically accessing a computer in an office somewhere. As the California Legislature worried then, an employee could misuse his employer's computer by "accessing computer data to use in a term paper." RJN Ex. 2 at 8 (S.B. 255, Bill Analysis, S. Comm. on Jud., Reg. Sess. (Cal. 1987-88)).

Thirty years later, the statutory provisions do not define the offenses with sufficient

definiteness. For example, the California law criminalizes "[k]nowingly and without permission us[ing] or caus[ing] to be used computer services." Cal. Penal Code § 502(c)(3). "Computer services" is defined as "includ[ing], but is not limited to, computer time, data processing, or storage functions, Internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(4). The permutations of criminalized conduct are now virtually endless. A person who sends an email from a friend's laptop without permission is a criminal. A brother who snoops on his sister's cell phone is a criminal. A neighbor who uses another neighbor's Wi-Fi network without first asking is a criminal. A visitor who turns up an electronic thermostat while the host is in the bathroom is a criminal.

The Nevada law is no better. For example, it is criminal to modify (or any other number of expansive verbs) without authorization "any supporting documents which exist inside or outside a computer." Nev. Rev. Stat. § 205.4765(1). "Supporting documents" is not defined, and seemingly has no limitation as they can exist "inside or outside a computer." *Id.* The plain language of the statute therefore apparently criminalizes drawing a picture on someone else's user manual. It is even criminal to "attempt[] to obtain access to" "data" (*id.*), and "data" is defined as "a representation in any form of information, knowledge, facts, concepts or instructions which is being prepared or has been formally prepared and is intended to be processed, is being processed or has been processed in a system or network" (Nev. Rev. Stat. § 205.474). Thus, just *trying* to get access to *any* "knowledge" that *may be* processed in a computer would be criminal conduct. That is essentially meaningless.

These far-ranging applications of the criminal statutes are more than a hypothetical concern. Given the pervasiveness of computers in our modern commercial society, this Court must look beyond any "culpable behavior of the defendants before" it and instead "consider the effect on millions of ordinary citizens." *Nosal*, 676 F.3d at 862. A vague statutory provision is still unconstitutional even if "there is some conduct that clearly falls within the provision's grasp." *Johnson*, 135 S. Ct. at 2561. Thus, the existence of some "straightforward cases" under a vague law cannot render the law constitutional. *Id.* at 2560-61.

The statutory provisions also impermissibly "encourage arbitrary and discriminatory enforcement" (*Kolender*, 461 U.S. at 357) because there are hardly any bounds to the conduct that

falls under the statutes' purview. *See Nosal*, 676 F.3d at 860 ("Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement"). The statutes therefore violate due process because they lack "minimal guidelines" and vest absolute discretion in the hands of the prosecutor to determine what conduct is criminal. *See Morales*, 527 U.S. at 60-61; *Nosal*, 676 F.3d at 862. Moreover, the statutes allow the owner of the computer device (California) or the "victim" (Nevada) to bring civil actions, which means that private citizens can wield these amorphous criminal laws based on their own interests or whims—including, as here, as a weapon to suppress competition.[6]

2. The Statutes Are Unconstitutional As Applied To Rimini's Conduct

Even if the statutory provisions were facially constitutional, it would be unconstitutional to hold Rimini liable under these statutes for violating Oracle's website terms of use.

As a matter of federal due process, the en banc Ninth Circuit has rejected the position that "authorization" under an anti-hacking statute can be determined by reference to website terms of use. In *Nosal*, the government admitted that "without authorization" under the federal anti-hacking statute was a "prohibition [that] applies to hackers," but contended that it could establish an individual "exceed[ed] authorized access" by violating computer terms of use. 676 F.3d at 857-58. The en banc Ninth Circuit disagreed: "Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." *Id.* at 860. The problem is that "[w]henever we access a web page, … we are using one computer to send commands to other computers at remote locations. Our access to those remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands." *Id.* at 861. As the court colorfully illustrated, premising criminal liability on website terms of use could lead to absurd results: "posting for sale an item prohibited by Craigslist's policy, or describing yourself [on eHarmony] as 'tall, dark and handsome,' when you're

[6] The remarkable vagueness of these statutes is illustrated by Oracle's request for an injunction. Oracle requests the Court to enjoin Rimini from "access[ing] (including download[ing] from) any Oracle website in any manner that could damage, disable, overburden, impair, or otherwise result in unauthorized access to or interference with, the proper functioning of any Oracle accounts, systems, or networks, including but not limited to access by or use of any automated or computerized method simulating manual downloading." Dkt. 900-1 at 16. Yet simply visiting a website could "overburden" it, since websites can handle only so much traffic, and the phrasing of "could" does not even require that such access *actually* overburden a website.

actually short and homely, will earn you a handsome orange jumpsuit." *Id.* at 862. The constitutional problems identified by the Ninth Circuit in *Nosal* apply with equal force to the state laws under the Due Process Clause of the Fourteenth Amendment. *See* U.S. Const., art. XIV; *see*, *e.g.*, *Morales*, 527 U.S. at 46, 61 (striking vague city ordinance under Fourteenth Amendment).

The due process concerns are heightened by the fact that private parties can unilaterally change their website terms of use (as Oracle did here), meaning that "behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever." *Nosal*, 676 F.3d at 862. In short, "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 860; *see United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009) ("basing a [federal anti-hacking] misdemeanor violation … upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine").

The Ninth Circuit in *Nosal* avoided these serious constitutional concerns by interpreting the federal law in a way that did not prohibit the conduct at issue there. This Court should do the same. *See*, *e.g.*, *Zadvydas*, 533 U.S. at 689 (canon of constitutional avoidance); *see Ashwander v. TVA*, 297 U.S. 288, 348 (1936) (Brandeis, J., concurring) (same). These constitutional concerns can be avoided by interpreting the prohibited conduct not to reach Rimini's use of an automated downloading tool, or by interpreting "permission" and "authorization" as not requiring specific authorization for such use from the website owner. *See supra* Section IV.B.[7]

Even if the California subsections could be applied to *accessing* a website, premising criminal liability based on violation of website terms of use raises the same constitutional problems. For example, in *Facebook*, 2010 U.S. Dist. LEXIS 93517, the court determined that "allowing violations of terms of use to fall within the ambit of the statutory term 'without permission' does essentially place in private hands unbridled discretion to determine the scope of criminal liability recognized

[7] The Nevada law has parallel language to the federal law insofar as both require access "without authorization." Nev. Rev. Stat. § 205.4765; 18 U.S.C. § 1030(a). The due process problems with the identical statutory language identified in *Nosal* apply equally to the Nevada law, and, correspondingly, a lack of "authorization" under the Nevada anti-hacking statute cannot be premised on violation of website terms of use.

under the statute." *Id.* at *28. Thus, the court held that "interpreting the statutory phrase 'without permission' in a manner that imposes liability for a violation of a term of use or receipt of a cease and desist letter would create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use." *Id.* at *33. Accordingly, "to avoid rendering the statute constitutionally infirm," the court held "that a user of internet services does not access or use a computer, computer network, or website without permission simply because that user violated a contractual term of use." *Id.* at *34; *see also Enki Corp. v. Freedman*, 2014 U.S. Dist. LEXIS 9169, at *9-10 (N.D. Cal. Jan. 23, 2014) (rejecting claim that "a violation of the established terms of use is sufficient to create liability").

D. $14.4 Million Of The Damages Award Cannot Be Sustained

In addition to the $27,000 in actual response costs incurred by Oracle, the jury awarded $14.4 million in lost profits on the hacking claims. Yet neither statute authorizes the recovery of lost profits. Even if lost profits were available, that award is completely unsupported by the evidence. Thus, even if the liability verdicts could be sustained, the damages must be reduced by $14.4 million.

1. The Statutes Do Not Authorize The Recovery Of Lost Profits

The California statute specifically delineates the compensatory damages available under the statute, but does not include lost profits. It states that "[c]ompensatory damages *shall include* any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502(e)(1) (emphasis added). The statute elsewhere references section 502(e)(1)'s definition of compensatory damages. *Id.* § 502.01(g)(1) (victim may elect "compensatory damages, *as defined* in paragraph (1) of subdivision (e) of Section 502") (emphasis added).

The plain language of that definition limits the available compensatory damages to the measures specified in the statute. The term "includes" can be used "as a word of limitation or as a word of enlargement." *Coast Oyster Co. v. Perluss*, 218 Cal. App. 2d 492, 501 (1963). When, as here, it is followed by "specific and detailed" language, courts interpret it as a word of limitation. *Pitney-Bowes, Inc. v. State of California*, 108 Cal. App. 3d 307, 317 (1980); *see Coast Oyster*, 218 Cal. App. 2d at 501-02; *In re Martinez*, 56 Cal. App. 2d 473, 477-78 (1942). A limiting

interpretation is particularly appropriate when the Legislature elsewhere in the statute uses the phrase "including, but not limited to" (*Coast Oyster*, 218 Cal. App. 2d at 501-02), as it has here. *See* Cal. Penal Code § 502(b)(2), (4), (5), (12). And, to the extent ambiguity exists, the rule of lenity requires a "construction which is more favorable to the offender." *People v. Davis*, 29 Cal. 3d 814, 828 (1981). In short, compensatory damages are limited to the measures specified in the statute.[8]

The structure of the statute also supports this interpretation. The statute defines "injury" as harm to computer systems. Cal. Penal Code § 502(b)(10) ("'Injury' means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program"). The statute then allows for a civil action to recover compensatory damages to compensate for that injury (i.e., actual harm to computer systems), plus the defined investigation costs. *Id.* § 502(e)(1). Nothing in the plain text or structure of the statute authorizes the award of subsequent attenuated economic damages such as lost profits far removed from computer harm.

The legislative history also reflects an intent to limit compensatory damages to the specified forms of relief. The original bill defined "injury" as (1) actual harm to computers, and (2) investigation costs: "'Injury' means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access." RJN Ex. 1 (S.B. 255 (Cal., as introduced Jan. 28, 1987)). In response to a memorandum from the Deputy District Attorney (*id.* Ex. 4), the Legislature divided that definition into "injury" for harm to computers and "victim expenditure" for investigation costs, for purposes of clarifying the distinction between a misdemeanor and a felony. Those definitions were passed and remain in the law today. Cal. Penal Code § 502(b)(10), (11). The civil recovery position, drafted as part of the same legislation, therefore contemplated economic recovery for the same categories of

[8] In comparison, the Legislature knows how to use the phrase "shall include" as one of enlargement rather than limitation. *See*, *e.g.*, Cal. Bus. & Prof. Code § 17029 ("shall include *without limitation* …"); Cal. Welfare & Inst. Code § 5328(e) ("shall include, *but need not be limited to*, …"); Cal. Labor Code § 139.6 ("shall include, *but not be limited to*, …") (emphases added).

harm recognized by the statute: "injury" and "expenditures," both defined by statute. *Id.* § 502(e)(1).

The Nevada anti-hacking statute allows for recovery of "[d]amages for any response costs, loss or injury suffered as a result of the crime." Nev. Rev. Stat. § 205.511. "Response costs" are defined as "reasonable costs" that generally relate to investigating, determining the amount of damage, remedying or preventing future damage, and testing or restoring the system. *Id.* § 205.4759. The plain language therefore limits damages to investigation costs and damages that are directly attributable to "the crime"—in other words, damages that result *directly* from the unauthorized access. Nothing in the plain language or structure allows for the recovery of lost profits.

Although the case law interpreting the California and Nevada statutes is sparse (or, in Nevada's case, nonexistent), this question has arisen many times under the federal anti-hacking law, and it is clear that lost profits are not recoverable under that statute. *See Farmers Ins. Exchange v. Steele Ins. Agency, Inc.*, 2013 U.S. Dist. LEXIS 104606, at *59 (E.D. Cal. July 25, 2013) ("costs not related to computer impairment or computer damages are not compensable") (collecting cases); *see also Instant Tech., LLC v. DeFazio*, 40 F. Supp. 3d 989, 1019 (N.D. Ill. 2014) (same); *Sprint Solutions, Inc. v. Pac. Cellupage Inc.*, 2014 U.S. Dist. LEXIS 101397, at *14-15 (C.D. Cal. July 21, 2014) (same). As the courts have explained, "economic losses," such as lost profits or harm to a business, "are better addressed under state contract and trade secrets law" because they are too attenuated from computer impairment or computer damages. *Steele, Ins. Agency*, 2013 U.S. Dist. LEXIS at *59 (quoting *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009)); *see Sprint Solutions*, 2014 U.S. Dist. LEXIS 101397, at *14-15 ("costs that are only distantly related to intrusions into a computer network are not losses under the [statute]").[9]

The same rationale applies with equal force to the state laws. Like the federal law, the state statutes allow for recovery of compensatory damages flowing from damage or loss as a result of the prohibited conduct. And, like the federal law, those compensatory damages must be related directly

[9] This Court recognized that the federal anti-hacking statute does not allow for the recovery of lost profits when it rejected Oracle's attempt to include such damages in the final jury instructions. *Compare* Dkt. 868 at 94-95 (Rimini's proposed modifications to remove item #6 of lost profits as a recoverable damage), *with* Final Jury Instructions, sent via email Oct. 5, 2015 ("Federal Computer Fraud and Abuse Act – Damages" instruction) (item #6 removed).

to actual computer impairment or damage. Lost profits are too attenuated from the harm against which the statutes protect. *Cf. Steele, Ins. Agency*, 2013 U.S. Dist. LEXIS at *59; *Sprint Solutions*, 2014 U.S. Dist. LEXIS 101397, at *15. Accordingly, the statutes do not authorize the recovery of lost profits, and the jury's award of $14.4 million in lost profits must be stricken.

2. The Lost Profits Award Is Unsupported By Legally Sufficient Evidence

Even if lost profits were legally available under the statutes, the jury's award of lost profits is unsupported by *any* evidence in the trial record.

Oracle offered nothing but a conclusory and demonstrably illogical theory for lost profits. According to Oracle, it suffered $14.4 million of lost profits as follows: (1) Mr. Hicks identified customer IDs used by Rimini in the three-month period, (2) Ms. Dean checked to see if those same customers were in her copyright lost profits analysis for Oracle International Corporation, and (3) if they were, Ms. Dean added up the copyright lost profits damages she had calculated for those customers. 9/24 Tr. 1832:21-1833:19. That number ($14.4 million) emerged for the first time at trial and was not in Ms. Dean's damages report, but it is what the jury awarded.

That damages award cannot be upheld because Oracle made *no attempt* to explain *how* it lost profits from automated downloading. There is no basis in the trial record upon which it can be concluded that Rimini's use of a customer's ID to download support materials caused Oracle to lose all profits for that customer. The record demonstrated that there were many different reasons customers left Oracle. *E.g.*, 9/22 Tr. 1339:19-21, 1317:15-17, 1302:5-22, 1335:17-1336:2; 9/23 Tr. 1518:2-11. And Oracle did not provide evidence of *one* customer who left *because of* Rimini's automated downloading from November 2008 to January 2009.

Moreover, these speculative lost profits are completely unsustainable in the face of a jury verdict awarding Oracle $0 in lost profits under the Copyright Act. Oracle's request for $14.4 million was a *subset* of Oracle's overall *copyright* lost profits analysis for *Oracle International Corporation*. 9/24 Tr. 1832:21-1833:12. The jury's finding confirms what the trial record makes clear: Oracle's causation theory that every Oracle customer would have renewed its contract with Oracle but for Rimini's conduct was based on impermissible speculation that the jury plainly rejected because each customer left Oracle for individual reasons. Indeed, Oracle's experts *admitted* that they

did not conduct *any* analysis regarding whether specific customers left Oracle because of any specific action related to unauthorized access. 9/24 Tr. 1861:2-22. The record therefore cannot support an award of a *single penny* of lost profits for unauthorized downloading from November 2008 to January 2009 because, without any causal nexus whatsoever, the award is purely speculative. *See*, *e.g.*, *Mackie v. Rieser*, 296 F.3d 909, 915 (9th Cir. 2002) (there must be "a legally sufficient causal link between" a violation and lost profits); *Lewis Jorge Constr. Mgmt., Inc. v. Pomona Unified School Dist.*, 34 Cal. 4th 960, 969-77 (2004) (rejecting award of "potential profits lost from future contracts" in breach-of-contract claim as "too speculative," in part because such damages must be "caused by the breach of contract"); *see generally People v. Morris*, 46 Cal. 3d 1, 21 (1988) ("A finding of fact must be an inference drawn from evidence rather than … mere speculation"), *overruled on other grounds by In re Sassounian*, 9 Cal. 4th 535, 543, n.5-6 (1995). Moreover, the jury awarded Oracle $35.6 million for its copyright infringement claim, so any award of copyright lost profits under the anti-hacking statutes is an impermissible duplicative recovery.[10]

E. Rimini Is Entitled To Judgment As A Matter Of Law On Oracle's UCL Claim

The Court should reject Oracle's request for judgment on its UCL claim (Dkt. 900 at 25), and instead grant judgment to Rimini. The UCL "borrows violations of other laws and treats them as unlawful practices." *Cel-Tech Comms., Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999) (citation omitted); Cal. Bus. & Prof. Code § 17200. Oracle dropped many of its claims and the jury rejected others, and the only predicate act left for which Oracle seeks relief under the UCL is the California anti-hacking law. Dkt. 900 at 25. But, as set forth above, the jury's liability finding under the California anti-hacking statute should be vacated. And without a predicate act, Oracle's UCL claim must fail too. *E.g.*, *Synopsys, Inc. v. Atoptech, Inc.*, 2013 U.S. Dist. LEXIS 153089, at *46-47 (N.D. Cal. Oct. 24, 2013) (dismissing UCL claim based on California anti-hacking statute when

[10] Oracle's attempt to recover copyright lost profits through anti-hacking statutes also leads to federal preemption of those statutes under the Copyright Act. 17 U.S.C. § 301(a); *e.g.*, *Johnson v. Arista Holding, Inc.*, 2006 U.S. Dist. LEXIS 88152, at *22 (S.D.N.Y. Dec. 5, 2006) ("Common law causes of action are generally preempted when they seek damages that are identical to those sought for copyright infringement"); *Firoozye v. Earthlink Network*, 153 F. Supp. 2d 1115, 1130 (N.D. Cal. 2001) ("where a plaintiff is only seeking damages [on a state law claim] from a defendant's reproduction of a work … the claim is preempted").

dismissing claim based on California anti-hacking statute). In addition, just as Oracle International Corporation lacks standing to assert the claim (*see supra* Section IV.A.1), it also lacks standing to assert a UCL claim. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 959-61 (9th Cir. 2009).[11]

Oracle is not entitled to restitution, because restitution is not available when, like here, "the plaintiff's remedies at law are adequate." *Collins v. eMachs., Inc.*, 202 Cal. App. 4th 249, 260 (2011); *see Dairy Queen v. Wood*, 369 U.S. 469, 478 (1962). Oracle has adequate remedies at law under the California anti-hacking statute, which is premised on the same injury. *See*, *e.g.*, *Am. Gen. Life & Accident Ins. Co. v. Findley*, 2013 U.S. Dist. LEXIS 41644, at *44-48 (C.D. Cal. Mar. 15, 2013) (equitable relief unavailable when a duplicative or redundant remedy is pursued to redress the same injury); *Stationary Eng'rs Local 39 Health & Welfare Trust Fund v. Philip Morris, Inc.*, 1998 U.S. Dist. LEXIS 8302, at *56 (N.D. Cal. Apr. 30, 1998) (same). And Oracle has not proven any amount to which it would be entitled. *See In re Tobacco Cases II*, 240 Cal. App. 4th 779, 792-802 (2015) (plaintiff did not provide substantial evidence to support UCL restitution).[12]

V. CONCLUSION

The Court should enter judgment as a matter of law for Rimini on Oracle's claims under state anti-hacking laws, the UCL, unfair practices, equitable restitution, and an accounting.[13]

DATED: November 13, 2015

GIBSON, DUNN & CRUTCHER LLP

By: *Blaine H. Evanson*
Blaine H. Evanson

Attorneys for Defendants

---

[11] Oracle's UCL claim is also preempted by the Copyright Act because the relief it seeks is entirely duplicative of its claims for copyright damages. 17 U.S.C. § 301(a); *Del Madera Props. v. Rhodes & Gardner, Inc.*, 820 F.2d 973, 977 (9th Cir. 1987). Oracle premised its "hacking" theory of recovery on the exact same theory of lost profit damages as its copyright claims (9/24 Tr. 1832:21-1833:12; note 10 and accompanying text, *supra*), and its attempt to recover the same lost profits under a theory of equitable restitution is preempted. *See Del Madera*, 820 F.2d at 977; *Gashtili v. JB Carter Props. II, LLC*, 2013 WL 1752808, *4 (D. Nev. Apr. 23, 2013).

[12] Oracle's request for an injunction fails as a matter of law because Oracle has an adequate legal remedy and for the other reasons set forth in Rimini's injunction opposition. *See* Dkt. 906.

[13] Oracle abandoned its claims for unfair practices (Cal. Bus. & Prof. Code § 17000) and an accounting (Dkt. 146 ¶¶ 155-62) by not pressing them at trial (rightly so, because those claims are legally unsupported (*e.g.*, Dkt. 838)), and judgment is warranted in Rimini's favor on those claims. *E.g.*, *Hunt v. City of L.A.*, 523 F. App'x 493, 495 (9th Cir. 2013). Oracle's separate claim for restitution (Dkt. 146 ¶¶ 152-54) fails for the same reasons as its UCL claim for restitution.

CERTIFICATE OF SERVICE

I hereby certify that on November 13, 2015, I caused to be electronically filed the foregoing document with the clerk of the court for the U.S. District Court, District of Nevada, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

By: *Blaine H. Evanson*
Blaine H. Evanson

Attorney for Defendants
Rimini Street, Inc. and Seth Ravin